AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of using a peer-to-peer type resolution to enable a secured, centralized hierarchical lookup between connected devices, the method comprising:

generating one or more first cryptographic keys associated with a first namespace of a first domain, the first domain being a member of a set of centralized hierarchical domains of namespaces;

creating a first authority using one of the one or more first cryptographic keys;

generating one or more next cryptographic keys associated with a next higher-level namespace, the next higher-level namespace at a higher level domain than the first namespace, the higher level domain being another member of the set of centralized hierarchical domains of namespaces;

creating a next higher-level authority using one of the one or more next cryptographic keys; and

publishing, using the peer-to-peer type resolution, an association between the first and the next higher-level namespaces, the association comprising:

a signed resolution that resolves a unique name of the first namespace to the first authority,

the signed resolution signed with the one of the one or more next cryptographic keys and the unique name including the next higher-level authority and the first namespace.

2. (Original) The method of claim 1 wherein the connected devices are part of a peer-to-peer network cloud.

3. (Canceled)

4. (Previously presented) The method of claim 1, further comprising: if the first namespace comprises a service, publishing a second association, the second association comprising a signed service resolution that resolves the first authority to an end result that

provides data, the signed service resolution signed with the one of the one or more first cryptographic keys.

5. (Previously presented) The method of claim 1, further comprising: if the first namespace comprises a service, publishing a second association, the second association comprising a signed service resolution that resolves the first authority to an IP address, a protocol name and a port, the signed service resolution signed with the one of the one or more first cryptographic keys.

6. (Previously presented) The method of claim 1 further comprising: supporting a dynamic change of address of the first namespace from an initial to a new address via delegating authority, comprising publishing, using the peer-to-peer type resolution, a new association between the new address and the first namespace, the new association comprising a signed new resolution that resolves the first authority to the new address, the signed new resolution signed with the one of the one or more first cryptographic keys.

7. (Previously presented) The method of claim 1 wherein the signed resolution resolves the name to one of the group: a host and a service.

8. (Previously presented) The method of claim 1 wherein creating the first authority includes performing a first hash of the one of the one or more first cryptographic keys, the one of the one or more first cryptographic keys being a first public key from a first private key-public key pair, and

wherein creating the next higher-level authority includes performing a next hash of the one of the one or more next cryptographic keys, the one of the one or more next cryptographic keys being a next public key from a next private key-public key pair.

9-18. (Canceled)

19. (Currently Amended) A method of generating a data structure for implementing a name resolution protocol, comprising:

generating a first field comprising a first authority component associated with a first public key, the first public key being part of a first private key-public key pair and the first authority component corresponding to a first namespace of a first domain, the first domain a member of a set of centralized, hierarchical namespaces; and

generating a second field comprising a second name component associated with a second namespace, the second namespace corresponding to a second authority and a domain of the second namespace being another member of the set of centralized, hierarchical namespaces and being at a lower level than a domain of the first namespace, wherein the first authority component and the second name component are capable of resolving to ~~a~~ the second authority, and

providing the generated data structure to the name resolution protocol for publishing a resolution that resolves the first authority component and the second name component to the second authority.

20. (Previously presented) The method of claim 19, further comprising: if the second namespace is a service, providing the second authority component to the name resolution protocol for publishing a second resolution that resolves the second authority to a port number, a protocol name, and an IP address of the service.

21. (Previously presented) The method of claim 19, wherein if the first namespace is a first host, the first authority component and the second name component are capable of resolving to a second host corresponding to the second authority.

22. (Previously presented) The method of claim 19, further comprising retrieving one or more from the group an IP address, a protocol name, and a port number from a cache.

23. (Currently Amended) A computer readable storage medium tangibly embodying a program of instruction executable by a computer for performing steps for using a peer-to-peer type resolution to enable a secured, centralized hierarchical lookup between connected devices, the steps comprising:

generating one or more first cryptographic keys associated with a first namespace of a first domain, the first domain being a member of a set of centralized hierarchical domains of namespaces;

creating a first authority using one of the one or more first cryptographic keys;

generating one or more next cryptographic keys associated with a next higher-level namespace, the next higher-level namespace at a higher-level domain than the first namespace, the higher level domain being another member of the set of centralized hierarchical domains of namespaces;

creating a next higher-level authority using one of the one or more next cryptographic keys; and

publishing, using the peer-to-peer type resolution, an association between the first and the next higher-level namespaces, the association comprising:

a signed resolution that resolves a unique name of the first namespace to the first authority,

the signed resolution signed with the one of the one or more next cryptographic keys and the unique name including the next higher-level authority and the first namespace.

24. (Previously presented) The computer readable storage medium of claim 23 wherein the connected devices are part of a peer-to-peer network cloud.

25. (Canceled)

26. (Previously presented) The computer readable storage medium of claim 23 wherein if the first namespace is a service, publishing a second association, the second association comprising a signed service resolution of the first authority to one or more of: arbitrary data or the group of an IP address, a protocol name and a port, the signed service resolution signed with the one of the one or more first cryptographic keys.

27. (Previously presented) The computer readable storage medium of claim 23 wherein the steps further comprise: supporting a dynamic change of address of the first namespace from an initial to a new address via delegating the authority, comprising publishing, using the peer-to-peer type resolution, a new association between the new address and the first namespace, the new association comprising a signed new resolution that resolves the first authority to the new address, the signed new resolution signed with the one of the one or more first cryptographic keys.

28. (Previously presented) The computer readable storage medium of claim 23 wherein the signed resolution resolves the name to one of the group: a host and a service.

29. (Previously presented) The computer readable storage medium of claim 23 wherein the signed resolution resolves the name to arbitrary data.

30. (Previously presented) The computer readable storage medium of claim 23 wherein creating the first authority includes performing a first hash of the one of the one or more first cryptographic keys, the one of the one or more first cryptographic keys being a first public key from a first private key-public key pair, and

wherein creating the next higher-level authority includes performing a next hash of the one of the one or more next cryptographic keys, the one of the one or more next cryptographic keys being a next public key from a next private key-public key pair.

31-38. (Canceled)